(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년04월29일
(11) 등록번호 10-2391952
(24) 등록일자 2022년04월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/06* (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/083 (2013.01)
H04L 9/0618 (2013.01)
(21) 출원번호 10-2021-0074113
(22) 출원일자 2021년06월08일
심사청구일자 2021년06월08일
(56) 선행기술조사문헌
JP11249825 A*
(뒷면에 계속)

(73) 특허권자
주식회사 에이치에스엠클라우디피아
서울특별시 강서구 공항대로 228, 1001호 (마곡동, 리더스타워마곡)
(72) 발명자
이종휘
부산광역시 북구 금곡대로 166, 504동 2903호 (화명동, 롯데캐슬카이저)
박세준
경기도 김포시 풍무로68번길 39, 105동 502호(풍무동, 한화유로메트로아파트)
김준모
서울특별시 강서구 방화대로5다길 34-5, 403호(공항동, 태경럭셔리하우스)
(74) 대리인
특허법인(유한)케이비케이

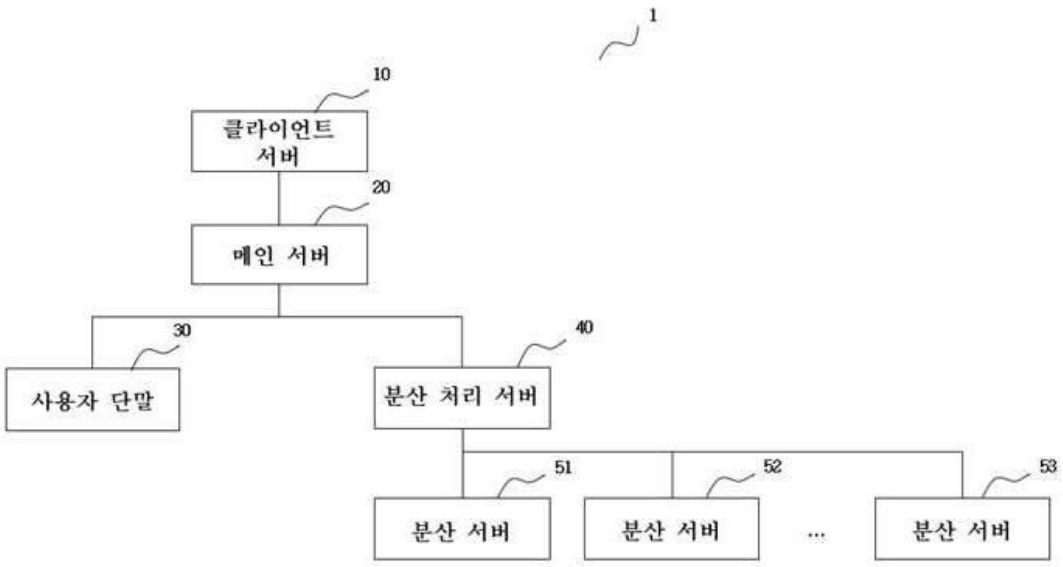
전체 청구항 수 : 총 6 항 심사관 : 나용수

(54) 발명의 명칭 **암호화 분산 처리 시스템, 장치 또는 이를 위한 방법**

(57) 요 약

본 발명은 암호화 분산 처리 시스템을 제안하고자 하며, 해당 시스템은 클라이언트 서버; 메인 서버; 사용자 단말; 분산 처리 서버; 및 복수의 분산 서버를 포함하며, 키 또는 암호화 패스워드 등을 분할하여 보관하고 키와 암호화 패스워드의 분할 방식도 알 수가 없으므로, 완전한 키 또는 암호화 패스워드를 획득하기가 매우 어렵고, 완전한 키 또는 암호화 패스워드를 획득하더라도 복호화 모듈은 클라이언트 서버만 보유하므로 클라이언트 서버 외의 다른 주체는 암호화 패스워드의 복호화가 불가능한 암호화 또는 복호화 방안을 제공한다.

대 표 도



(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/302 (2013.01)

(56) 선행기술조사문헌
JP2007272583 A*
KR101792220 B1*
KR102010776 B1*
KR1020200134744 A*
Jong-Phil Yang 외 2명, "A Simplified Approach to User Controllable Threshold Signatures", IEEE (2004.)*
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

암호화 분산 처리 시스템에 있어서,

키(key)를 생성하고, 생성된 키와 패스워드(password), 그리고 사용자 식별정보를 메인 서버로 전송하고, 상기 키와 패스워드를 상기 메인 서버로 전송하고 나면, 상기 키 및 상기 패스워드를 삭제하는 클라이언트 서버;

상기 클라이언트 서버로부터 상기 키와 상기 패스워드, 그리고 상기 사용자 식별정보를 수신하고, 암호화 모듈을 이용하여 상기 수신된 키로 상기 패스워드를 암호화하며, 상기 키와 암호화된 패스워드 각각을 미리 설정된 분할 방식 중 하나를 이용하되, 상기 키를 분할하기 위한 방식과 상기 패스워드를 분할하기 위한 방식은 서로 다른 방식을 이용하여 적어도 둘로 분할하여, 적어도 하나의 분할키, 적어도 하나의 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제1 블록을 사용자 단말로 전달하고, 나머지 분할키, 나머지 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제2 블록을 분산 처리 서버로 전송하고, 상기 제1 블록 및 상기 제2 블록을 전송하고 나면, 상기 분할키 및 분할 암호화 패스워드를 제거하는 메인 서버;

상기 메인 서버로부터 상기 제1 블록을 수신하고, 상기 제1 블록에 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 제1 식별정보를 할당하고, 상기 제1 블록에 포함된 분할키 및 분할 암호화 패스워드를 RSA(Rivest Shamir Adleman) 암호화한 후 저장하는 사용자 단말; 및

상기 메인 서버로부터 상기 제2 블록을 수신하고, 상기 제2 블록에 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 상기 제1 식별정보와 상이한 제2 식별정보를 할당하고, 상기 제2 블록에 포함된 분할키 및 분할 암호화 패스워드 각각을 미리 결정된 수 또는 미리 결정된 크기로 분할하고, 상기 분할된 분할키 및 분할 암호화 패스워드를 미리 결정된 수의 서브 블록으로 분산처리하여 하나 이상의 분산 서버에 저장하게 하는 분산 처리 서버를 포함하고,

상기 미리 설정된 분할 방식은 분할의 수 또는 크기, 분할의 구성 및 분할된 키와 암호화 패스워드 상호 간의 순서 중 적어도 하나에 대한 설정을 포함하고,

상기 미리 설정된 분할 방식에 따라 상기 사용자 단말 및 상기 분산 처리 서버로 전달된 분할키 및 분할 암호화 패스워드가 결정되고,

상기 미리 결정된 수의 서브 블록은 서로 다른 독립된 값의 식별정보를 할당받는, 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

암호화 분산 처리 시스템에 있어서,

사용자 식별정보를 포함하는, 암호화 패스워드의 전달 요청을 전송하는 클라이언트 서버;

상기 클라이언트 서버로부터 상기 암호화 패스워드의 전달 요청을 수신하여, 사용자 단말 및 복수의 분산 서버 또는 상기 복수의 분산 서버를 관리하는 분산 처리 서버로 암호화 패스워드의 전달 요청을 전송하는 메인 서버;

상기 암호화 패스워드의 전달 요청에 따라, 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 제1 식별정보가 할당된, RSA 암호화된 제1 분할키 및 제1 분할 암호화 패스워드를 포함한 제1 블록을 상기 메인 서버로 전송하고, 상기 제1 블록을 전송하고 나면 상기 제1 블록을 삭제하는 사용자 단말;

상기 암호화 패스워드의 전달 요청에 따라, 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 상기 제1 식별정보와 상이한 제2 식별정보가 할당된, 상기 복수의 분산 서버에 분산 처리된 제2 분할키 및 제2 분할 암호화 패스워드를 포함한 제2 블록의 미리 결정된 수의 서브 블록을 회수한 후 결합하여 제2 블록을 획득하고, 획득된 제2 블록을 상기 메인 서버로 전송하고, 상기 제2 블록을 전송하고 나면 상기 제2 블록을 삭제하는 분산 처리 서버를 포함하고,

여기서, 상기 제1 분할키와 상기 제2 분할키는 미리 설정된 분할 방식 중 제1 미리 설정된 분할 방식을 이용하여 키를 분할하여 획득되며, 상기 제1 분할 암호화 패스워드 및 상기 제2 분할 암호화 패스워드는 상기 미리 설정된 분할 방식 중 제2 미리 설정된 분할 방식을 이용하여 패스워드를 분할하여 획득되며, 상기 제1 미리 설정된 분할 방식과 상기 제2 미리 설정된 분할 방식은 서로 다른 방식이고,

상기 메인 서버는:

상기 RSA 암호화된 제1 블록을 RSA 복호화하여 제1 분할키 및 제1 분할 암호화 패스워드를 획득하고, 상기 제1 미리 설정된 분할 방식에 기초하여 상기 제1 분할키 및 상기 제2 분할키를 결합하고, 상기 제2 미리 설정된 분할 방식에 기초하여 상기 제1 분할 암호화 패스워드 및 상기 제2 분할 암호화 패스워드를 결합하여, 키와 암호화 패스워드를 획득하고, 상기 획득된 키와 상기 획득된 암호화 패스워드를 상기 클라이언트 서버로 전송하고 상기 획득된 키와 상기 획득된 암호화 패스워드를 전송하고 나면 상기 획득된 키와 상기 획득된 암호화 패스워드를 삭제하며,

상기 클라이언트 서버는 복호화 모듈을 이용하여 상기 획득된 키로 상기 획득된 암호화 패스워드를 복호화하고,

상기 미리 설정된 분할 방식은 분할의 수 또는 크기, 분할의 구성 및 분할된 키와 암호화 패스워드 상호 간의 순서 중 적어도 하나에 대한 설정을 포함하고,

상기 미리 설정된 분할 방식에 따라 상기 사용자 단말 및 상기 분산 처리 서버로 전달된 분할키 및 분할 암호화 패스워드가 결정되고,

상기 미리 결정된 수의 서브 블록은 서로 다른 독립된 값의 식별정보를 할당받는, 시스템.

청구항 11

암호화 분산 처리 방법에 있어서,

키(key)를 생성하고, 생성된 키와 패스워드(password), 그리고 사용자 식별정보를 수신하는 단계;

암호화 모듈을 이용하여 상기 수신된 키로 상기 패스워드를 암호화하며, 상기 키와 상기 암호화된 패스워드 각각을, 미리 설정된 분할 방식 중 하나를 이용하되 상기 키를 분할하기 위한 방식과 상기 패스워드를 분할하기

위한 방식은 서로 다른 방식을 이용하여, 적어도 둘로 분할하는 단계; 및

제1 분할키, 제1 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제1 블록을 사용자 단말로 전송하고, 나머지 분할키, 나머지 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제2 블록을 분산 처리 서버로 전송하고, 상기 제1 블록 및 상기 제2 블록을 전송하고 나면, 상기 분할키 및 상기 암호화 패스워드를 삭제하는 단계를 포함하고,

상기 제1 블록은 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 제1 식별정보를 할당받고, 상기 제1 블록에 포함된 제1 분할키 및 제1 분할 암호화 패스워드는 RSA(Rivest Shamir Adleman) 암호화된 후 상기 사용자 단말에 저장되며,

상기 제2 블록은 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 제1 식별정보와 상이한 제2 식별정보를 할당받고, 상기 제2 블록에 포함된 나머지 분할키 및 나머지 분할 암호화 패스워드 각각은 미리 결정된 수 또는 미리 결정된 크기로 분할된 후, 상기 분할된 분할키 및 분할 암호화 패스워드를 미리 결정된 수의 서브 블록으로 분산처리되어 상기 분산 처리 서버가 관리하는 하나 이상의 분산 서버에 저장되고,

상기 미리 설정된 분할 방식은 분할의 수 또는 크기, 분할의 구성 및 분할된 키와 암호화 패스워드 상호 간의 순서 중 적어도 하나에 대한 설정을 포함하고,

상기 미리 설정된 분할 방식에 따라 상기 사용자 단말 및 상기 분산 처리 서버로 전달된 분할키 및 분할 암호화 패스워드가 결정되고,

상기 미리 결정된 수의 서브 블록은 서로 다른 독립된 값의 식별정보를 할당받는, 방법.

청구항 12

암호화 분산 처리 방법에 있어서,

사용자 식별정보를 포함하는 클라이언트 서버로부터 암호화 패스워드의 전달 요청을 수신하는 단계;

사용자 단말 및 복수의 분산 서버 또는 상기 복수의 분산 서버를 관리하는 분산 처리 서버로 암호화 패스워드의 전달 요청을 전송하는 단계;

상기 암호화 패스워드의 전달 요청에 대응하여, 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 제1 식별정보가 할당된, RSA 암호화된 제1 분할키 및 제1 분할 암호화 패스워드를 포함한 제1 블록을 상기 사용자 단말로부터 수신하고, 미리 결정된 함수를 이용하여 상기 사용자 식별정보에 기반한 상기 제1 식별정보와 상이한 제2 식별정보가 할당된, 상기 복수의 분산 서버에 분산 처리된 제2 분할키 및 제2 분할 암호화 패스워드를 포함한 제2 블록의 미리 결정된 수의 서브 블록을 회수한 후 결합하여 획득된 제2 블록을 상기 분산 처리 서버로부터 수신하는 단계, 상기 제1 블록은 상기 사용자 단말에서 전송되고 나면 상기 사용자 단말에서 삭제되고 상기 제2 블록은 상기 분산 처리 서버에서 전송되고 나면 상기 분산 처리 서버에서 삭제됨; 및

여기서, 상기 제1 분할키와 상기 제2 분할키는 미리 설정된 분할 방식 중 제1 미리 설정된 분할 방식을 이용하여 키를 분할하여 획득되며, 상기 제1 분할 암호화 패스워드 및 상기 제2 분할 암호화 패스워드는 상기 미리 설정된 분할 방식 중 제2 미리 설정된 분할 방식을 이용하여 패스워드를 분할하여 획득되며, 상기 제1 미리 설정된 분할 방식과 상기 제2 미리 설정된 분할 방식은 서로 다른 방식이고,

상기 RSA 암호화된 제1 블록을 RSA 복호화하여 제1 분할키 및 제1 분할 암호화 패스워드를 획득하고, 상기 제1 미리 설정된 분할 방식에 기초하여 상기 제1 분할키 및 상기 제2 분할키를 결합하고, 상기 제2 미리 설정된 분할 방식에 기초하여 상기 제1 분할 암호화 패스워드 및 상기 제2 분할 암호화 패스워드를 결합하여, 키와 암호화 패스워드를 획득하고, 상기 획득된 키와 상기 획득된 암호화 패스워드를 상기 클라이언트 서버로 전송하고 상기 획득된 키와 상기 획득된 암호화 패스워드를 전송하고 나면 상기 획득된 키와 상기 획득된 암호화 패스워드를 삭제하는 단계를 포함하고,

상기 클라이언트 서버로 전송된 암호화 패스워드는 복호화 모듈을 이용하여 상기 획득된 키로 복호화되고,

상기 미리 설정된 분할 방식은 분할의 수 또는 크기, 분할의 구성 및 분할된 키와 암호화 패스워드 상호 간의 순서 중 적어도 하나에 대한 설정을 포함하고,

상기 미리 설정된 분할 방식에 따라 상기 사용자 단말 및 상기 분산 처리 서버로 전달된 분할키 및 분할 암호화

패스워드가 결정되고,

상기 미리 결정된 수의 서브 블록은 서로 다른 독립된 값의 식별정보를 할당받는, 방법.

청구항 13

제11항에 따른 방법을 수행하기 위한 컴퓨터 판독가능한 매체에 저장된 컴퓨터 프로그램.

청구항 14

제12항에 따른 방법을 수행하기 위한 컴퓨터 판독가능한 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 암호화 분산 처리 시스템, 장치 또는 이를 위한 방법에 관한 것으로서, 패스워드(password)를 암호화하고 분산 처리 또는 저장하는 것에 관한 발명이다.

배 경 기 술

[0002] 인터넷 또는 모바일 서비스의 발달로 인해 대부분의 사람들은 인터넷을 통해 정부기관, 교육기관, 의료기관, 통신회사, 금융회사, 포털, 소셜네트워크서비스(Social Network Service; SNS), 게임, 쇼핑 등의 수많은 온라인 서비스를 이용한다.

[0003] 따라서, 이러한 서비스를 이용하고자 하는 사용자는 자신의 실명 등을 포함한 개인정보를 입력하여 회원에 가입하거나, 사용자 식별정보(identification; ID)와 패스워드를 입력하여 가입된 사용자임을 인증해야 한다. 또한, 온라인 서비스의 주체 별로 이러한 사용자의 정보, 즉 ID와 패스워드 등을 저장해놓아야, 사용자 인증이 가능하다.

[0004] 그러나, 온라인 서비스의 주체 별로 이러한 사용자의 정보의 저장은, 즉 집중화는 정보의 유출 위험에 노출되게 된다. 즉, 온라인 서비스의 주체 중 어느 하나만 해킹이 이루어지면, 해당 온라인 서비스 뿐만 아니라 다른 온라인 서비스에도 불법적인 또는 악의적인 접근이 가능해진다.

[0005] 이를 위해, 사용자의 정보를 암호화하고 분산 처리하여, 해킹의 위험을 제거하기 위한 암호화 분산 시스템, 장치 또는 방법 등을 제안하고자 한다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 사용자 정보의 유출의 위험을 제거하기 위한, 암호화 분산 시스템, 장치 또는 방법을 제안하고자 한다.

[0007] 본 발명에서 이루고자 하는 해결하고자 하는 과제들은 상기 해결하고자 하는 과제로 제한되지 않으며, 언급하지 않은 또 다른 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시예에 따른 암호화 분산 처리 시스템에 있어서, 상기 시스템은 키(key)를 생성하고, 생성된 키와 패스워드(password), 그리고 사용자 식별정보를 메인 서버로 전송하는 클라이언트 서버; 상기 클라이언트 서버로부터 상기 키와 상기 패스워드, 그리고 상기 사용자 식별정보를 수신하고, 암호화 모듈을 이용하여 상기 수신된 키로 상기 패스워드를 암호화하며, 상기 키와 암호화된 패스워드 각각을 적어도 둘로 분할하여, 적어도 하나의 분할키, 적어도 하나의 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제1 블록은 사용자 단말로 전달하고, 나머지 분할키, 나머지 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제2 블록은 분산 처리 서버로 전송하는 메인 서버; 상기 메인 서버로부터 상기 제1 블록을 수신하고, 상기 제1 블록에 포함된 분할키 및 분할 암호화 패스워드를 RSA(Rivest Shamir Adleman) 암호화한 후 저장하는 사용자 단말; 및 상기 메인 서버로부터 상기 제2 블록을 수신하고, 상기 제2 블록에 포함된 분할키 및 분할 암호화 패스워드를 미리

결정된 수의 서브 블록으로 분산처리하여 하나 이상의 분산 서버에 저장하게 하는 분산 처리 서버를 포함할 수 있다.

[0009] 추가로 또는 대안으로, 상기 클라이언트 서버는 상기 키와 패스워드를 상기 메인 서버로 전송하고 나면, 상기 키 및 상기 패스워드를 삭제할 수 있다.

[0010] 추가로 또는 대안으로, 상기 메인 서버는 상기 제1 블록 및 상기 제2 블록을 전송하고 나면, 상기 분할키 및 분할 암호화 패스워드를 제거할 수 있다.

[0011] 추가로 또는 대안으로, 상기 메인 서버는 미리 설정된 분할 방식 중 하나를 이용하여 상기 키와 상기 암호화 패스워드를 분할할 수 있다.

[0012] 추가로 또는 대안으로, 상기 미리 설정된 분할 방식은 분할의 수 또는 크기, 분할의 구성 및 분할된 키와 암호화 패스워드 상호 간의 순서 중 적어도 하나에 대한 설정을 포함할 수 있다.

[0013] 추가로 또는 대안으로, 상기 분산 처리 서버는 상기 제2 블록에 포함된 분할키 및 분할 암호화 패스워드 각각을 미리 결정된 수 또는 미리 결정된 크기로 분할할 수 있다.

[0014] 추가로 또는 대안으로, 상기 사용자 단말은 미리 결정된 함수를 이용하여 제1블록에 포함된 분할키와 분할 암호화 패스워드에 상기 사용자 식별정보에 기반한 제1 식별정보를 할당할 수 있다.

[0015] 추가로 또는 대안으로, 상기 분산 처리 서버는 미리 결정된 함수를 이용하여 제2 블록에 포함된 분할키와 분할 암호화 패스워드에 상기 사용자 식별정보에 기반한 제2 식별정보를 할당할 수 있다.

[0016] 추가로 또는 대안으로, 상기 제2 식별정보는 상기 제1 식별정보와 상이할 수 있다.

[0017] 본 발명의 또다른 일 실시예에 따른 암호화 분산 처리 시스템에 있어서, 상기 시스템은 암호화 패스워드의 전달을 요청하는 클라이언트 서버; 상기 클라이언트 서버로부터 상기 암호화 패스워드의 전달 요청을 수신하여, 사용자 단말 및 복수의 분산 서버 또는 상기 복수의 분산 서버를 관리하는 분산 처리 서버로 암호화 패스워드의 전달을 요청하는 메인 서버; 상기 암호화 패스워드의 전달 요청에 따라, RSA 암호화된 제1 분할키 및 제1 분할 암호화 패스워드를 포함한 제1 블록을 상기 메인 서버로 전송하는 사용자 단말; 상기 암호화 패스워드의 전달 요청에 따라, 상기 복수의 분산 서버에 분산 처리된 제2 분할키 및 제2 분할 암호화 패스워드를 포함한 제2 블록의 서브 블록을 회수한 후 결합하여 제2 블록을 획득하고, 획득된 제2 블록을 상기 메인 서버로 전송하는 분산 처리 서버를 포함하고, 상기 메인 서버는 상기 RSA 암호화된 제1 블록을 RSA 복호화하여 제1 분할키 및 제1 분할 암호화 패스워드를 획득하고, 상기 제1 분할키 및 상기 제2 분할키를 결합하고, 상기 제1 분할 암호화 패스워드 및 상기 제2 분할 암호화 패스워드를 결합하여, 키와 암호화 패스워드를 획득하고, 상기 획득된 키와 상기 획득된 암호화 패스워드를 상기 클라이언트 서버로 전송하고, 상기 클라이언트 서버는 복호화 모듈을 이용하여 상기 획득된 키로 상기 획득된 암호화 패스워드를 복호화할 수 있다.

[0018] 본 발명의 또다른 일 실시예에 따른 암호화 분산 처리 방법에 있어서, 상기 방법은 키(key)를 생성하고, 생성된 키와 패스워드(password), 그리고 사용자 식별정보를 수신하는 단계; 암호화 모듈을 이용하여 상기 수신된 키로 상기 패스워드를 암호화하며, 상기 키와 상기 암호화된 패스워드 각각을 둘로 분할하는 단계; 및 제1 분할키, 제1 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제1 블록은 사용자 단말로 전달하고, 제2 분할키, 제2 분할 암호화 패스워드 및 상기 사용자 식별정보를 포함하는 제2 블록은 분산 처리 서버로 전달하는 단계를 포함하고, 상기 제1 블록에 포함된 제1 분할키 및 제1 분할 암호화 패스워드는 RSA(Rivest Shamir Adleman) 암호화된 후 상기 사용자 단말에 저장되며, 상기 제2 블록에 포함된 제2 분할키 및 제2 분할 암호화 패스워드는 미리 결정된 수의 서브 블록으로 분산처리되어 상기 분산 처리 서버가 관리하는 하나 이상의 분산 서버에 저장될 수 있다.

[0019] 본 발명의 또다른 일 실시예에 따른 암호화 분산 처리 방법에 있어서, 클라이언트 서버로부터 암호화 패스워드의 전달 요청을 수신하는 단계; 사용자 단말 및 복수의 분산 서버 또는 상기 복수의 분산 서버를 관리하는 분산 처리 서버로 암호화 패스워드의 전달을 요청하는 단계; 상기 암호화 패스워드의 전달 요청에 대응하여, RSA 암호화된 제1 분할키 및 제1 분할 암호화 패스워드를 포함한 제1 블록을 수신하고, 상기 복수의 분산 서버에 분산 처리된 제2 분할키 및 제2 분할 암호화 패스워드를 포함한 제2 블록을 수신하는 단계; 및 상기 RSA 암호화된 제1 블록을 RSA 복호화하여 제1 분할키 및 제1 분할 암호화 패스워드를 획득하고, 상기 제1 분할키 및 상기 제2 분할키를 결합하고, 상기 제1 분할 암호화 패스워드 및 상기 제2 분할 암호화 패스워드를 결합하여, 키와 암호화 패스워드를 획득하고, 상기 획득된 키와 상기 획득된 암호화 패스워드를 상기 클라이언트 서버로 전송하는

단계를 포함하고, 상기 클라이언트 서버로 전송된 암호화 패스워드는 복호화 모듈을 이용하여 상기 획득된 키로 복호화될 수 있다.

[0020] 또한, 본 발명의 또다른 실시예에 따라, 앞서 설명한 방법을 수행하기 위한 컴퓨터 판독가능한 매체에 저장되는 컴퓨터 프로그램이 제안된다.

[0021] 상기 과제 해결방법들은 본 발명의 실시예들 중 일부에 불과하며, 본원 발명의 기술적 특징들이 반영된 다양한 실시예들이 당해 기술분야의 통상적인 지식을 가진 자에 의해 이하 상술할 본 발명의 상세한 설명을 기반으로 도출되고 이해될 수 있다.

발명의 효과

[0022] 본 발명에 따르면 키와 패스워드를 안전하게 보관할 수 있는 효과가 있다.

[0023] 좀더 상세하게는, 본 발명에 따르면 키와 패스워드를 분할하여 여러 곳에 나누어 보관하므로, 키와 패스워드가 분할되어 저장된 모든 곳에서 분할키 또는 분할 암호화 패스워드가 유출되지 않는 한, 완전한 키 또는 암호화 패스워드의 획득이 불가능하다.

[0024] 본 발명에서 얻은 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0025] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

도 1은 본 발명에 따른 암호화 분산 처리 시스템의 구성도를 도시한다.

도 2는 본 발명에 따른 암호화 과정의 순서도를 도시한다.

도 3은 본 발명에 따른 복호화 과정의 순서도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 본 발명의 실시예를 첨부한 도면을 참고하여 설명한다. 그러나 본 발명은 본 명세서에서 설명하는 실시예에 한정되지 않으며 여러 가지 다른 형태로 구현될 수 있다. 본 명세서에서 사용되는 용어는 실시예의 이해를 돕기 위한 것이며, 본 발명의 범위를 한정하고자 의도된 것이 아니다. 또한, 이하에서 사용되는 단수 형태들은 문구들이 이와 명백히 반대의 의미를 나타내지 않는 한 복수 형태들도 포함한다.

[0027] 도 1은 본 발명에 따른 암호화 분산 처리 시스템(1)의 구조도를 도시한다.

[0028] 본 발명에 따른 암호화 분산 처리 시스템(1)은 클라이언트 서버(10), 메인 서버(20), 사용자 단말(30), 분산 처리 서버(40) 및 하나 이상의 분산 서버(50)를 포함할 수 있다.

[0029] 먼저 암호화 과정에 대해 설명하도록 한다. 암호화 과정은 사용자의 패스워드 저장 시도를 통해 개시될 수 있다.

[0030] 클라이언트 서버(10)는 사용자의 패스워드 저장 시도를 검출할 수 있다. 이에, 클라이언트 서버(10)는 메인 서버(20)와 약속된 키(key)를 생성할 수 있다. 또는 메인 서버(20)와 약속된 키가 클라이언트 서버(10)에 사전에 주어질 수 있다. 약속된 키는 미리 결정된 크기를 가질 수 있으며, 난수 생성 함수를 통해 생성될 수 있다.

[0031] 클라이언트 서버(10)는 복호화 모듈을 이용하거나 보유할 수 있다. 복호화 모듈은 사용자 정보, 또는 그 중에서 암호화된 패스워드(이하, “암호화 패스워드”로 지칭함)를 복호화하기 위한 것으로서, 약속된 키와 암호화 패스워드를 입력받으면 (암호가 해독된)패스워드를 출력할 수 있다. 여기서, 복호화 모듈은 메인 서버(20)가 이용하거나 보유하는 암호화 모듈과는 상응 또는 대칭적인 관계로서, 약속된 키와 암호화 모듈을 이용하여 암호화된 패스워드는 약속된 키와 복호화 모듈을 이용하여 복호화가 가능하다.

[0032] 클라이언트 서버(10)와 메인 서버(20)는 API(application programming interface) 통신을 통해 정보, 데이터 또는 메시지를 송수신할 수 있다. 클라이언트 서버(10)와 메인 서버(20)가 API 통신을 하기 위해서는 1회성 토큰이 필요하다. 클라이언트 서버(10)는 미리 발급받은 키 값으로 메인 서버(20)로 토큰 값을 요청하고, 메인

서버(20)는 미리 발급한 키 값과 클라이언트 서버(10)의 서버 IP 주소를 비교하여, API 통신을 통제할 수 있다.

[0033] 클라이언트 서버(10)는 약속된 키, (사용자) 패스워드, 그리고 사용자 식별정보(ID)를 메인 서버(20)로 전송할 수 있다. 이 때, 클라이언트 서버(10)는 약속된 키, 패스워드 및 사용자 식별정보를 저장하지 않는다. 즉, 클라이언트 서버(10)가 약속된 키, 패스워드 및 사용자 식별정보를 메인 서버(20)로 전송하고 나면, 약속된 키, 패스워드 및 사용자 식별정보는 클라이언트 서버(10) 혹은 클라이언트 서버(10) 내 저장소 등에서 삭제될 수 있다. 이는 클라이언트 서버(10)에서 키 또는 패스워드와 같은 정보 유출의 가능성을 제거하기 위함이고, 결국엔 키 및 패스워드의 보안성이 강화되는 효과가 있다.

[0034] 메인 서버(20)는 클라이언트 서버(10)로부터 약속된 키, (사용자) 패스워드, 그리고 사용자 식별정보를 수신할 수 있다. 메인 서버(20)는 클라이언트 서버(10)가 이용하거나 보유하는 복호화 모듈과 상응 또는 대칭적인 암호화 모듈을 이용하거나 보유할 수 있다. 메인 서버(20)는 암호화 모듈을 이용하여 약속된 키로 패스워드를 암호화할 수 있다. 이에 따라, 암호화 패스워드가 생성될 수 있다. 또한, 패스워드의 암호화가 완료되면, 메인 서버(20)에는 클라이언트 서버(10)로부터 수신된 패스워드가 더 이상 존재하지 않을 수 있다.

[0035] 그리고나서, 메인 서버(20)는 약속된 키와 암호화 패스워드 각각을 미리 설정된 분할 방식 중 하나를 이용하여 분할할 수 있다. 약속된 키와 암호화 패스워드의 분할(암호화하기 전의 패스워드의 분할 포함)을 위한 미리 설정된 분할 방식은 분할의 수 또는 크기, 분할의 구성 및 분할된 키와 암호화 패스워드 상호 간의 순서 중 적어도 하나에 대한 설정 또는 정함 등을 포함할 수 있다. 분할의 수 또는 크기, 구성 및 순서 등에 따른 구체적인 분할 방식은 좀더 상세히 설명하도록 한다.

[0036] 메인 서버(20)는 약속된 키와 암호화 패스워드 각각을 미리 결정된 수로 분할하거나, 또는 미리 결정된 크기를 갖도록 분할할 수 있다. 즉, 메인 서버(20)는 약속된 키를 N개로 분할, 그리고 암호화 패스워드를 M개로 분할할 수 있다(N과 M 각각은 2이상의 정수이고, 같을 수도 있고 다를 수도 있다).

[0037] 예컨대, 메인 서버(20)는 약속된 키와 암호화 패스워드 각각을 둘로 분할할 수 있다. 즉, 메인 서버(20)는 약속된 키를 제1 분할키 및 제2 분할키로 분할하고, 암호화 패스워드를 제1 분할 암호화 패스워드 및 제2 분할 암호화 패스워드로 분할할 수 있다. 암호화 패스워드의 분할은 본 발명의 시스템 내의 여러 구성에 나누어 보관 또는 저장하게끔 하여 시스템 구성 중 일부가 해킹이 되더라도, 약속된 키 또는 패스워드를 복구 또는 복호화하지 못하게 하기 위함이다.

[0038] 예컨대, 약속된 키가 64자리의 문자로 구성되고(즉, 문자열), 약속된 키가 둘로 분할되는 경우, 메인 서버(20)는 약속된 키의 가장 높은 자리(가장 좌측의 문자)부터 32개의 문자를 제1 분할키로, 나머지 32개의 문자를 제2 분할키로 분할할 수 있다.

[0039] 암호화 패스워드에 대한 분할 역시, 위에서 설명한 약속된 키에 대한 분할과 동일한 방식으로 수행될 수 있다. 예컨대, 암호화 패스워드가 200자리의 문자열로 구성되고 암호화 패스워드가 둘로 분할되는 경우, 메인 서버(20)는 암호화 패스워드의 가장 높은 자리부터 100개의 문자를 제1 분할 암호화 패스워드로, 나머지 100개의 문자를 제2 분할키로 분할할 수 있다.

[0040] 아래의 표는 키와 패스워드가 각각 18자리의 문자인 경우의 키와 패스워드의 분할을 동일한 방식으로 수행한 결과의 예시를 나타낸다.

표 1

[0041]

키와 패스워드	키:abcdefghi123456789 암호화 패스워드:abcdefghi123456789
제1 분할키	abcdefghi
제1 암호화 패스워드	abcdefghi
제2 분할키	123456789
제2 암호화 패스워드	123456789

[0042] 또는, 약속된 키가 64자리의 문자열로 구성된 경우, 메인 서버(20)는 가장 높은 자리의 문자와, 그로부터 한 문자를 건너뛰어 선택된 32개의 문자를 제1 분할키로, 나머지 문자를 제2 분할키로 분할할 수 있다(즉, 64개의 문자 중 짝수 번째 문자의 조합 또는 결합을 하나의 분할키로, 홀수 번째 문자의 조합 또는 결합을 나머지 하나의 분할키로 분할함).

[0043] 암호화 패스워드가 200자리의 문자열로 구성된 경우, 메인 서버(20)는 가장 높은 자리의 문자와, 그로부터 한 문자를 건너뛰어 선택된 100개의 문자를 제1 분할 암호화 패스워드로, 나머지 100개의 문자를 제2 분할 암호화 패스워드로 분할할 수 있다(즉, 200개의 문자 중 짝수 번째 문자의 조합 또는 결합을 하나의 분할 암호화 패스워드로, 홀수 번째 문자의 조합 또는 결합을 나머지 하나의 분할 암호화 패스워드로 분할함).

[0044] 아래의 표는 키와 패스워드가 각각 18자리의 문자인 경우의 키와 패스워드의 분할을 동일한 방식으로 수행한 결과의 예시를 나타낸다.

표 2

[0045]

키와 패스워드	키:abcdefghi123456789 암호화 패스워드:abcdefghi123456789
제1 분할키	acegi2468
제1 암호화 패스워드	acegi2468
제2 분할키	bdfh13579
제2 암호화 패스워드	bdfh13579

[0046] 표 1과 2에서는, 키와 패스워드를 서로 동일한 방식으로 분할하는 예를 설명하였지만, 키와 패스워드는 서로 다른 방식으로 분할될 수 있을 것이다. 예컨대, 키는 표 1에서 예시한 방식대로 분할하고, 패스워드는 표 2에서 예시한 방식대로 분할할 수 있다.

[0047] 또한, 위에서 설명한 약속된 키와 암호화 패스워드가 분할되는 수 또는 정도(N, M)가 3 이상으로 설정되면, 분할 방식이 더욱 다양해질 수 있다. 예컨대, 약속된 키가 64자리의 문자열로 구성되고, 3개로 분할되어야 하는 경우, 64개 자리의 문자를 가장 높은 자리부터 하나씩을 순환적으로 이동(cyclic shift)하면서 선택하여 3개의 분할키로 분할하는 방법이 사용될 수 있다. 분할되는 수가 약속된 키 또는 암호화 패스워드의 전체 자리수의 약수가 아니면(즉, 나누어떨어지지 않으면), 각 분할키 또는 분할 암호화 패스워드의 길이 또는 크기는 서로 동일하지 않을 수 있다.

[0048] 또한, 위에서 설명한 약속된 키와 암호화 패스워드가 분할되는 수 또는 정도(N, M)가 서로 다를 수도 있다.

[0049] 예컨대, 약속된 키는 두 개로 분할되나(제1 분할키 및 제2 분할키), 암호화 패스워드는 세 개로 분할될 수 있다(제1 분할 암호화 패스워드, 제2 분할 암호화 패스워드 및 제3 분할 암호화 패스워드). 이 경우에도, 분할 방식은 상술한 바를 참조할 수 있다.

[0050] 이러한 분할 방식을 알 수 없으면, 분할키와 분할 암호화 패스워드를 획득하더라도, 완전한 약속된 키 및 암호화 패스워드를 복구할 수 없을 것이다.

[0051] 한편, 분할키 또는 분할 암호화 패스워드는 사용자 단말(30)과 분산 처리 서버(40)로 전달되므로, 분할키 또는 분할 암호화 패스워드 상호간의 순서 역시 중요할 수 있다. 예컨대, 약속된 키가 64자리의 문자열로 구성되는 경우, 사용자 단말(30)로 전달될 제1 분할키와 분산 처리 서버(40)로 전달될 제2 분할키의 상대적인 위치, 즉 순서는 메인 서버(20)의 분할 방식에 따라 달라질 수 있다.

[0052] 앞서 설명한 표 1과 2의 예에서는, 약속된 키의 전체 문자열에서 가장 높은 자리(가장 좌측)의 문자부터 일정 개수의 문자들 또는 짝수 번째 문자들을 사용자 단말(30)로 전송하는 제1 분할키로 지칭하고, 그 나머지 문자들을 분산 처리 서버(40)로 전송하는 제2 분할키로 지칭하였으나, 이 순서는 반대로 구성될 수 있다. 즉, 약속된 키의 전체 문자열에서 가장 높은 자리(가장 좌측)의 문자부터 일정 개수의 문자들 또는 짝수 번째 문자들을 분산 처리 서버(40)로 전송하는 제1 분할키로 지칭하고, 그 나머지 문자들을 사용자 단말(30)로 전송하는 제2 분할키로 지칭할 수 있다.

[0053] 이는 약속된 키 또는 암호화 패스워드의 분할되는 수 또는 정도가 커질수록 다양한 상호간의 순서가 가능하다. 약속된 키가 미리 설정된 수(예컨대, 3)로 분할되는 경우, 또는 사용자 단말(30)로 전송할 분할키의 크기가 약속된 키의 전체 문자열의 일부 비율(예컨대, 3분의 1)로 설정되는 경우, 제1 분할키, 제2 분할키 및 제3 분할키를 앞서 설명한 분할 구성에 따라 분할한 경우, 사용자 단말(30)이나 분산 처리 서버(40)로 어떤 분할키를 할당 또는 전송할 지가 결정될 수 있다. 예컨대, 사용자 단말(30)로 약속된 키의 전체 문자열의 3분의 1만을 전송해야 한다면, 메인 서버(20)는 3개의 분할키 중 어느 하나를 사용자 단말(30)로 전송할 것으로 결정하고, 나머지 분할키를 분산 처리 서버(40)로 전송할 것으로 결정할 수 있다.

[0054] 암호화 패스워드 또는 패스워드의 분할에 대해서도 분할키에 대해 설명한 순서에 대한 설명이 적용될 수 있다.

[0055] 이러한 상호 간의 순서를 알 수 없으면, 분할키와 분할 암호화 패스워드를 획득하더라도, 완전한 약속된 키 및 암호화 패스워드를 복구할 수 없을 것이다.

[0056] 따라서, 메인 서버(20)는 선택된 분할의 수 또는 크기, 분할의 구성 또는 분할된 키 또는 암호화 패스워드(또는 패스워드) 상호 간의 순서를 저장 또는 인지하고 있어야 하며, 선택된 분할의 수 또는 크기, 분할의 구성 또는 분할된 키 또는 암호화 패스워드(또는 패스워드) 상호 간의 순서 역시 암호화되는 등 보안 수단이 필요하다. 암호화 과정에서 이용된, 분할의 수 또는 크기, 분할의 구성 또는 분할된 키 또는 암호화 패스워드(또는 패스워드) 상호 간의 순서는 추후 암호화 분산 처리된 패스워드가 호출되는 경우에, 메인 서버(20)가 각 분산 처리 또는 저장된 키와 암호화 패스워드를 수집하게 되는데, 그 때 완전한 키 그리고 암호화 패스워드를 구성 또는 결합하기 위해 필요하다.

[0057] 요약하면, 약속된 키 또는 암호화 패스워드는 미리 설정된 방식 중 하나에 의해 분할될 수 있다. 즉, 약속된 키 또는 암호화 패스워드는 미리 결정된 크기 또는 수로 분할될 수 있으며, 미리 결정된 크기 또는 수는 약속된 키와 암호화 패스워드에 대해 서로 다를 수 있다. 또한, 약속된 키 또는 암호화 패스워드의 분할된 구성도 미리 결정된 구성에 따라 이루어 질 수 있으며, 분할키 또는 분할 암호화 패스워드 상호 간의 순서 역시 미리 결정된 순서에 따라 결정될 수 있다.

[0058] 한편, 메인 서버(20)는 암호화 모듈을 이용하여 패스워드를 암호화하기 전에, 미리 설정된 다양한 방식 중 하나를 이용하여 패스워드를 분할할 수 있다. 여기서, 미리 설정된 다양한 방식은 앞서 약속된 키 또는 암호화 패스워드를 분할하는 과정과 관련하여 설명한 방식(즉, 분할 수 또는 크기, 분할 구성, 상호간의 순서 등)을 모두 포함할 수 있다.

[0059] 그 후, 메인 서버(20)는 약속된 키로 분할된 패스워드를 암호화 모듈을 이용하여 암호화할 수 있다. 이렇게 되면, 암호화 과정이 패스워드가 분할된 수 또는 정도만큼 수행될 수 있다. 약속된 키 역시 분할될 수 있으므로, 패스워드의 분할과 동시에 또는 그 이전, 이후에 메인 서버(20)는 미리 설정된 다양한 방식 중 하나를 이용하여 약속된 키를 분할할 수 있다. 여기서, 미리 설정된 다양한 방식은 앞서 암호화 패스워드를 분할하는 과정과 관련하여 설명한 방식을 포함할 수 있다. 이 때에도, 분할된 패스워드의 암호화가 완료되면, 메인 서버(20)에는 클라이언트 서버(10)로부터 수신된 패스워드가 더 이상 존재하지 않을 수 있다.

[0060] 메인 서버(20)는 분할된 약속된 키(즉, 분할키)와 분할된 암호화 패스워드(즉, 분할 암호화 패스워드)를 사용자 식별정보와 함께 사용자 단말(30)과 분산 처리 서버(40)로 전송할 수 있다. 메인 서버(20)가 약속된 키를 N개로 분할, 그리고 암호화 패스워드를 M개로 분할하거나 패스워드를 M개로 분할한 후 암호화한 경우, N개의 분할키 중 적어도 하나와 M개의 분할 암호화 패스워드 중 적어도 하나를 사용자 단말(30)로 전송하고, 나머지 분할키 및 분할 암호화 패스워드를 분산 처리 서버(40)로 전송할 수 있다.

[0061] 이 때, 메인 서버(20)는 키, 패스워드, 분할키, 분할 암호화 패스워드 및 사용자 식별정보를 저장하지 않는다. 즉, 메인 서버(20)가 분할키, 분할 암호화 패스워드 및 사용자 식별정보를 사용자 단말(30)과 분산 처리 서버(40)로 전송하고 나면, 분할키(클라이언트 서버(10)로부터 수신된 키 포함), 분할 암호화 패스워드(클라이언트 서버(10)로부터 수신된 패스워드 포함) 및 사용자 식별정보를 제거 또는 삭제 등을 하여, 메인 서버(20) 혹은 메인 서버(20) 내의 저장소 등에 패스워드, 분할키(클라이언트 서버(10)로부터 수신된 키 포함), 분할 암호화 패스워드 및 사용자 식별정보가 더 이상 존재하지 않도록 할 수 있다. 이는 메인 서버(20)에서 키, 패스워드, 분할키 또는 분할 암호화 패스워드와 같은 정보 유출의 가능성을 제거하기 위함이고, 결국엔 키 및 패스워드의 보안성이 강화되는 효과가 있다.

[0062] 사용자 단말(30)은 메인 서버(20)로부터 N개의 분할키 중 적어도 하나와 M개의 분할 암호화 패스워드 중 적어도 하나, 그리고 사용자 식별정보를 수신할 수 있다. 이하, 설명의 간단함을 위해, N개의 분할키 중 적어도 하나와 M개의 분할 암호화 패스워드 중 적어도 하나, 그리고 사용자 식별정보를 포함하는 정보 단위를 “제1 블록”으로 지칭하도록 한다. 사용자 단말(30)은 RSA(Rivest Shamir Adleman) 암호화 모듈을 이용하거나 보유할 수 있다. 이와 대응하게, 메인 서버(20)는 RSA 복호화 모듈을 이용하거나 보유할 수 있다. 메인 서버(20)와 사용자 단말(30)은 RSA 암, 복호화를 위한 RSA 키를 서로 공유할 수 있다.

[0063] 사용자 단말(30)은 RSA 암호화 모듈을 이용하여 수신된 제1 블록을 RSA 암호화할 수 있다. RSA 암호화가 완료되면, 사용자 단말(30)에는 메인 서버(20)로부터 수신된 제1 블록이 더 이상 존재하지 않을 수 있다. 그리고나서, 사용자 단말(30)은 RSA 암호화된 제1 블록을 로컬에 저장할 수 있다.

[0064] RSA 암호화된 제1 블록은 사용자 식별정보를 직접 포함하지 않고, 사용자 식별정보를 지시하는 방식으로 사용자 식별정보가 포함될 수 있다. 예를 들어, 제1 블록 내의 분할키와 분할 암호화 패스워드를 RSA 암호화한 파일명으로서 사용자 식별정보가 포함될 수 있다. 이 때, 파일명은 메인 서버(20)로부터 수신된 사용자 식별정보와는 다른 정보 또는 다른 값으로 할당될 수 있다. 즉, 사용자 단말(30)은 사용자 식별정보를 인코딩하는 별도의 함수를 이용하여 제1 식별정보를 생성하여, 제1 식별정보를 제1 블록에 할당할 수 있다.

[0065] 분산 처리 서버(40)는 메인 서버(20)로부터, 사용자 단말(30)로 전송되지 않은 나머지 분할키 및 나머지 분할 암호화 패스워드를 사용자 식별정보와 함께 수신할 수 있다. 이하, 설명의 간단함을 위해, 사용자 단말(30)로 전송되지 않은 나머지 분할키, 나머지 분할 암호화 패스워드 및 사용자 식별정보를 포함하는 정보 단위를 “제2 블록”으로 지칭하도록 한다. 분산 처리 서버(40)는 제2 블록을 수신하고 상기 제2 블록을 미리 결정된 수의 서브 블록으로 분산처리하여 하나 이상의 분산 서버(50)에 저장하게 할 수 있다. 분산 처리 과정을 통해, 제2 블록은 K개의 서브 블록으로 분할될 수 있으며(여기서 K는 2이상의 정수로서, 미리 설정될 수 있는 수이다), 또는 복수 개의 미리 설정된 크기의 서브 블록으로 분할될 수 있다. 각 서브 블록은 제2 블록에 포함된 분할키의 일부분 및 제2 블록에 포함된 분할 암호화 패스워드의 일부분을 포함하도록 구성될 수 있다. 이 때, 사용자 식별정보는 각 서브 블록의 파일명으로 저장될 수 있다. 즉, 분산 처리 서버(40) 는 메인 서버(20)로부터 수신된 사용자 식별정보를 인코딩하는 별도의 함수를 이용하여 제2 식별정보를 생성하여, 제2 식별정보를 제2 블록 또는 각 서브 블록에 할당할 수 있다. 각 서브 블록에 할당되는 제2 식별정보는 서로 다른 독립된 값을 가질 수 있다. 제2 식별정보와 사용자 식별정보 간의 연관관계에 대해서는, 분산 처리 서버(40)가 인식 또는 식별할 수 있도록 구성된다. 분산 처리가 되면, 분산 처리 서버(40)에는 메인 서버(20)로부터 수신된 제2 블록을 제거 또는 삭제 등을 하여, 제2 블록이 더 이상 존재하지 않도록 할 수 있다.

[0066] 또한, 분산 처리를 위해 분산 처리 서버(40) 또는 분산 서버(50)는 하둡(Hadoop) 시스템을 이용할 수 있다.

[0067] 앞서 설명한 대로, 키와 암호화 패스워드는 사용자 단말(30)과 분산 서버(50)에 분할되어 저장된다. 이에 따라 사용자 단말(30)과 분산 서버(50) 전부에서 해당 사용자의 분할키 및 분할 암호화 패스워드를 획득해야, 사용자의 완전한 키와 암호화 패스워드를 획득할 수 있다. 또한, 모든 분할키와 분할 암호화 패스워드를 획득하더라도, 전술한 다양한 분할 크기(수), 분할 구성, 분할키 또는 분할 암호화 패스워드의 상호간의 순서에 따라, 완전한 키와 암호화 패스워드를 재구성하는 것은 분할과 관련된 정보 없이는 불가능하다. 또한, 암호화 패스워드를 복호화하기 위한 복호화 모듈은 클라이언트 서버(10)에게만 있기 때문에, 클라이언트 서버(10)가 완전한 키와 암호화 패스워드를 가지고 있는 경우에만 복호화가 가능하다. 따라서, 클라이언트 서버(10)외의 다른 주체들은 완전한 키와 암호화 패스워드를 획득하여도, 복호화가 불가능하다. 따라서, 본 발명에 따르면 키의 패스워드와 관련하여 견고한 보안 체계를 구축할 수 있는 효과가 있다.

[0068] 본 발명에 따른 복호화 과정에 대해서 설명하도록 한다.

[0069] 복호화 과정은 사용자의 패스워드 호출에 따라 개시될 수 있다.

[0070] 클라이언트 서버(10)는 사용자의 패스워드 호출을 검출할 수 있다. 클라이언트 서버(10)는 암호화 과정에서 수신했던 키와 패스워드 및 사용자 식별정보를 모두 삭제했으므로, 더 이상 패스워드를 가지고 있지 않다. 이에, 클라이언트 서버(10)는 암호화 패스워드의 전달 요청을 메인 서버(20)에게 전송할 수 있다. 전달 요청에는 사용자 식별정보가 포함될 수 있고, 이에 누구를 위한 암호화 패스워드의 전달인지가 식별가능하다.

[0071] 메인 서버(20)는 암호화 패스워드의 전달 요청을 수신할 수 있다. 메인 서버(20)는 암호화 과정에서 수신했던 키와 패스워드 및 사용자 식별정보, 또는 분할키와 분할 암호화 패스워드를 더 가지고 있지 않다. 이에, 메인 서버(20)는 사용자 단말(30)과 분산 처리 서버(40)에게 암호화 패스워드의 전달 요청을 전송할 수 있다.

[0072] 사용자 단말(30)은 수신된 암호화 패스워드의 전달 요청에 따라, 로컬에 저장하고 있던 RSA 암호화된 제1 블록을 메인 서버(20)로 전송할 수 있다. 이 때, 사용자 단말(30)은 RSA 암호화된 제1 블록에서 사용자 식별정보를 추출할 수 있으며, 메인 서버(20)로 RSA 암호화된 제1 블록을 전송할 때, 추출된 사용자 식별정보를 함께 전송할 수 있다. 또한, 사용자 단말(30)은 RSA 암호화된 제1 블록을 메인 서버(20)로 전송하고 난 후에, RSA 암호화된 제1 블록을 제거 또는 삭제 등을 하여, 사용자 단말(30) 또는 사용자 단말(30) 내의 저장소 등에 RSA 암호화된 제1 블록이 더 이상 존재하지 않도록 할 수 있다.

[0073] 분산 처리 서버(40)는 수신된 암호화 패스워드의 전달 요청에 따라, 하나 이상의 분산 서버(50)로 암호화 패스워드의 전달 요청을 전송할 수 있다. 이에 대응하여, 각 분산 서버(50)는 제2 블록의 서브 블록을 분산 처리 서버(40)로 전송할 수 있다. 그리고, 분산 처리 서버(40)는 회수한 제2 블록의 서브 블록을 결합하여 제2 블록

을 다시 획득할 수 있고, 제2 블록을 메인 서버(20)로 전송할 수 있다. 이 때, 분산 처리 서버(40)는 제2 블록 또는 각 서브 블록에서 제2 식별정보에 기초하여 사용자 식별정보를 추출할 수 있으며, 메인 서버(20)로 제2 블록을 전송할 때, 추출된 사용자 식별정보를 함께 전송할 수 있다. 또한, 분산 처리 서버(40) 또는 각 분산 서버(50)는 제2 블록 또는 각 서브 블록을 전송하고 난 후에, 제2 블록 또는 각 서브 블록을 제거 또는 삭제 등을 하여 분산 처리 서버(40)와 각 분산 서버(50)에는 제2 블록 또는 각 서브 블록이 더 이상 존재하지 않도록 할 수 있다.

[0074] 또한, 메인 서버(20)는 사용자 단말(30)로부터 수신한 사용자 식별정보를 통해 클라이언트 서버(10)로부터의 전달 요청에 포함된 사용자 식별정보와 일치하는지를 확인할 수 있다. 또한, 메인 서버(20)는 분산 처리 서버(40)로부터 수신한 사용자 식별정보를 통해 클라이언트 서버(10)로부터의 전달 요청에 포함된 사용자 식별정보와 일치하는지를 확인할 수 있다. 당연하게도, 사용자 단말(30) 및 분산 처리 서버(40)로부터 수신된 사용자 식별정보가 클라이언트 서버(10)로부터의 전달 요청에 포함된 사용자 식별정보와 동일함이 확인되어야, 후술하는 과정이 계속될 수 있다.

[0075] 메인 서버(20)는 사용자 단말(30)로부터 수신한 RSA 암호화된 제1 블록을 RSA 복호화 모듈을 이용하여 복호화할 수 있다. 이로써, 메인 서버(20)에서 제1 블록이 획득될 수 있다. RSA 암호화된 제1 블록의 복호화가 완료되면, 메인 서버(20)에는 더 이상 RSA 암호화된 제1 블록이 존재하지 않을 수 있다.

[0076] 그 후, 메인 서버(20)는 제1 블록과 분산 처리 서버(40)로부터 수신된 제2 블록을 서로 결합할 수 있다. 제1 블록에는 적어도 하나의 분할키 및 적어도 하나의 분할 암호화 패스워드가 포함되어 있고, 제2 블록에는 나머지 분할키 및 나머지 분할 암호화 패스워드가 포함되어 있다. 다만, 앞서 상술한 바와 같이, 메인 서버(20)가 암호화 과정에서 제1 블록과 제2 블록을 다양한 방식 중 하나를 이용하여 분할하였으므로, 메인 서버(20)는 분할했던 방식을 이용하여 제1 블록과 제2 블록, 좀더 상세하게는 제1 블록에 포함된 분할키와 제2 블록에 포함된 분할키를 결합하고, 제1 블록에 포함된 분할 암호화 패스워드와 제2 블록에 포함된 분할 암호화 패스워드를 결합할 수 있다. 이에 따라, 메인 서버(20)에서 온전한 키와 암호화 패스워드가 획득된다. 그렇다 하여도, 메인 서버(20)는 암호화 모듈이 없으므로, 암호화 패스워드를 복호화할 수는 없다. 메인 서버(20)는 획득한 키와 암호화 패스워드를 클라이언트 서버(10)로 전송할 수 있다. 또한, 메인 서버(20)가 획득한 키와 암호화 패스워드를 클라이언트 서버(10)로 전송하고 난 후에는, 메인 서버(20)에는 키, 암호화 패스워드 그리고 제1 블록, 제2 블록은 더 이상 존재하지 않는다. 즉, 메인 서버(20)는 키와 암호화 패스워드 등을 제거하거나 삭제할 수 있다.

[0077] 클라이언트 서버(10)는 수신된 키를 이용하여 수신된 암호화 패스워드를 복호화할 수 있다. 이에 따라, 클라이언트 서버(10)에서 패스워드가 획득되며, 클라이언트 서버(10)는 사용자에게 패스워드를 반환할 수 있다. 또한, 클라이언트 서버(10)는 사용자에게 패스워드를 반환한 후에, 메인 서버(20)로부터 수신된 키와 암호화 패스워드를 삭제할 수 있다.

[0078] 도 2는 본 발명에 따른 암호화 분산 처리에 관련된 암호화 과정에 대한 순서도를 도시한다. 도 2에 도시된 과정은 메인 서버(20)에 의해 수행될 수 있다.

[0079] 메인 서버(20)는 키, 패스워드, 사용자 식별정보를 클라이언트 서버(10)로부터 수신할 수 있다(S210). 이 단계는 사용자의 패스워드 저장 시도에 따라 개시될 수 있다.

[0080] 메인 서버(20)는 수신된 키를 이용하여 패스워드를 암호화하는데(S220), 이때 암호화 모듈을 이용할 수 있다. 앞서 설명한 것처럼, 암호화 모듈은 클라이언트 서버(10)가 보유하거나 이용하는 복호화 모듈과 대응하는 것으로서, 암호화 모듈은 키를 이용하여 패스워드를 암호화할 수 있고, 복호화 모듈은 암호화 패스워드를 복호화할 수 있다. 암호화의 결과 암호화 패스워드가 획득될 수 있다.

[0081] 메인 서버(20)는 키와 암호화 패스워드 각각을 분할할 수 있다(S230). 분할의 방식은 앞서 설명한 다양한 분할 방식 중 하나를 이용할 수 있다. 키의 분할 및 암호화 패스워드의 분할을 통해 복수의 분할키 및 복수의 분할 암호화 패스워드가 획득될 수 있다.

[0082] 메인 서버(20)는 분할키와 분할 암호화 패스워드 중 일부는 사용자 단말(30)로 전송할 수 있고, 나머지는 분산 처리 서버(40)로 전송할 수 있다(S240).

[0083] 사용자 단말(30)로 전송된 일부 분할키와 일부 분할 암호화 패스워드(이하, “제1 블록”)는 사용자 단말(30)에서 RSA 암호화후 저장되며, 분산 처리 서버(40)로 전송된 나머지 분할키와 분할 암호화 패스워드(이하, “제2

블록”)는 분산 처리 서버(40)에서 분산처리된 후 하나 이상의 분산 서버(50)에 저장될 수 있다.

[0084] 이를 통해, 암호화 분산 처리 시스템(1)은 키 그리고 패스워드를 안전하게 암호화한 후 분산하여 저장할 수 있다.

[0085] 다음의 표는 사용자 단말(30)에서 제1 블록이 RSA 암호화되어 저장된 상태를 예시한다.

표 3

[0086]

평문	{
	KEY:abcdefghi,
	PASSWORD:abcdefghi
	}

RSA	10011001 1010100 10101 10101010 1010101 101010 010110 101010 01011 010101 01010

[0087] 아울러, 사용자 단말(30)은 로컬에 제1 블록은 다음과 같이 저장될 수 있다. 여기서, 사용자 식별정보는 test@tes.com이다.

표 4

[0088]

IDX: test@tes.com	10011001 1010100 10101 10101010 1010101 101010 010110 101010 01011 010101 01010

[0089] 도 2를 참조하여 설명되지 않은 암호화 과정에 대해서는 도 1을 참조하여 설명한 설명을 참조하도록 한다.

[0090] 도 3은 본 발명에 따른 암호화 분산 처리에 관련된 복호화 과정에 대한 순서도를 도시한다. 도 3에 도시된 과정은 메인 서버(20)에 의해 수행될 수 있다.

[0091] 메인 서버(20)는 클라이언트 서버(10)로부터 암호화 패스워드 전달 요청을 수신할 수 있다(S310). 이 단계는 사용자의 패스워드 호출 시도에 따라 개시될 수 있다.

[0092] 메인 서버(20)는 수신된 암호화 패스워드 전달 요청에 대응하여, 사용자 단말(30)과 분산 처리 서버(40)로 암호화 패스워드 전달 요청을 전송할 수 있다(S320).

[0093] 메인 서버(20)는 암호화 패스워드 전달 요청에 대응하여, 사용자 단말(30) 및 분산 처리 서버(40)로부터 분할키, 분할 암호화 패스워드 및 사용자 식별정보를 포함한 블록을 수신할 수 있다(S330).

[0094] 그 후, 메인 서버(20)는 수신된 암호화 블록을 처리하고, 처리된 암호화 블록에서 분할키들을 서로 결합하고, 분할 암호화 패스워드를 서로 결합하여, 키 및 암호화 패스워드를 획득할 수 있다(S340). 좀더 상세하게는, 메인 서버(20)는 사용자 단말(30)로부터 수신된 RSA 암호화 분할키 및 RSA 분할 암호화 패스워드로 구성된 RSA 암호화 제1 블록에 대해 RSA 복호화를 수행하여, 일부 분할키 및 일부 분할 암호화 패스워드로 구성된 제1 블록을 획득할 수 있다. 그리고 나서, 메인 서버(20)는 제1 블록의 일부 분할키 및 일부 분할 암호화 패스워드와, 분산 처리 서버(40)로부터 수신된 나머지 분할키 및 나머지 분할 암호화 패스워드, 즉 제2 블록을 결합하여, 키 및 암호화 패스워드를 획득할 수 있다. 분할키들의 결합, 그리고 분할 암호화 패스워드의 결합은 앞서 설명한 분할 방식에 대응하여 수행되어야 한다.

[0095] 메인 서버(20)는 획득된 키 및 암호화 패스워드를 클라이언트 서버(10)로 전송할 수 있다(S350). 클라이언트 서버(10)로 전송된 암호화 패스워드는 함께 전송된 키를 이용하여 복호화될 수 있다. 이를 통해, 클라이언트 서버(10)는 패스워드를 획득할 수 있고, 사용자에게 반환할 수 있다.

[0096] 도 3을 참조하여 설명되지 않은 복호화 과정에 대해서는 도 1을 참조하여 설명한 설명을 참조하도록 한다.

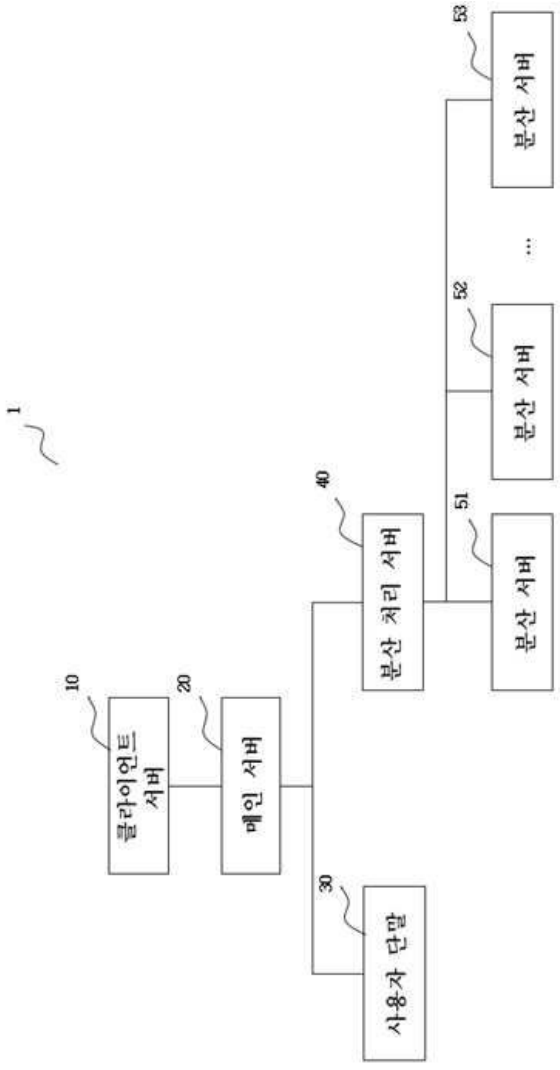
[0097] 이상의 명세서에서, “시스템”과 그에 속한 구성들(클라이언트 서버(10), 메인 서버(20), 사용자 단말(30), 분산 처리 서버(40), 분산 서버(50) 등)이 해당 방법 또는 절차 등을 수행하는 것으로 설명하였으나, "시스템"과 그에 속한 구성들은 명칭일 뿐 권리범위가 그에 종속되는 것은 아니다. 즉, 시스템 외에도 장치 등으로서도 해당 방법 또는 절차가 수행될 수 있으며, 그뿐만 아니라 분산 암호화 처리를 위한 소프트웨어 또는 컴퓨터 또는 그 밖의 기계, 장치 등으로 판독가능한 코드에 의해 상기 방법 또는 방식이 수행될 수 있다.

[0098] 아울러, 본 발명의 또다른 양태(aspect)로서, 앞서 설명한 제안 또는 발명의 동작이 "컴퓨터"(시스템 온 칩(system on chip; SoC) 또는 (마이크로) 프로세서 등을 포함하는 포괄적인 개념)에 의해 구현, 실시 또는 실행될 수 있는 코드 또는 상기 코드를 저장 또는 포함한 컴퓨터-판독가능한 저장 매체 또는 컴퓨터 프로그램 제품(product) 등으로도 제공될 수 있고, 본 발명의 권리범위가 상기 코드 또는 상기 코드를 저장 또는 포함한 컴퓨터-판독가능한 저장 매체 또는 컴퓨터 프로그램 제품으로 확장가능하다.

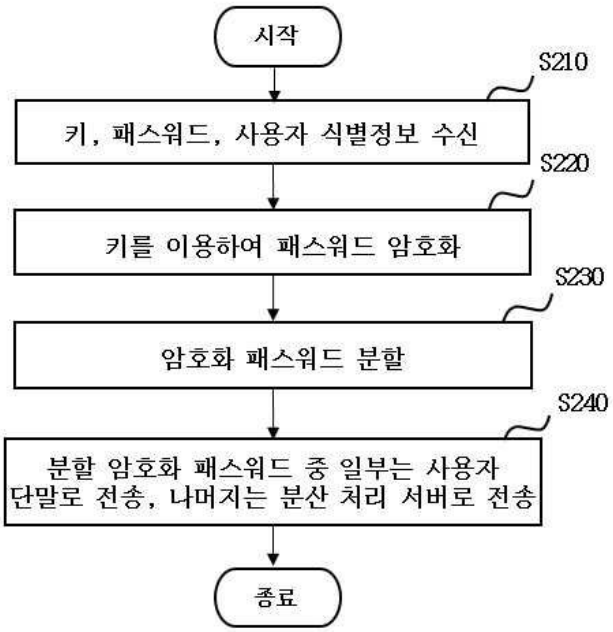
[0099] 상술한 바와 같이 개시된 본 발명의 바람직한 실시예들에 대한 상세한 설명은 당업자가 본 발명을 구현하고 실시할 수 있도록 제공되었다. 상기에서는 본 발명의 바람직한 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다. 따라서, 본 발명은 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다.

도면

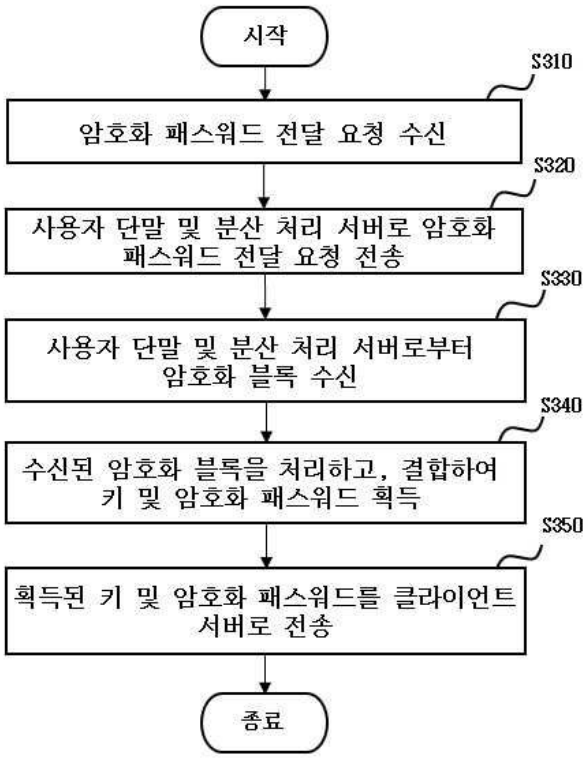
도면1



도면2


시작
S210
키, 패스워드, 사용자 식별정보 수신
S220
키를 이용하여 패스워드 암호화
S230
암호화 패스워드 분할
S240
분할 암호화 패스워드 중 일부는 사용자 단말로 전송, 나머지는 분산 처리 서버로 전송
종료

도면3


시작
S310
암호화 패스워드 전달 요청 수신
S320
사용자 단말 및 분산 처리 서버로 암호화 패스워드 전달 요청 전송
S330
사용자 단말 및 분산 처리 서버로부터 암호화 블록 수신
S340
수신된 암호화 블록을 처리하고, 결합하여 키 및 암호화 패스워드 획득
S350
획득된 키 및 암호화 패스워드를 클라이언트 서버로 전송
종료